UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

INTELLECTUAL VENTURES II LLC, Plaintiff, v. JP MORGAN CHASE & CO., et al., Defendants.	:	**ORDER AND OPINION DENYING MOTION FOR SUMMARY JUDGMENT BASED UPON NON-INFRINGEMENT** 13 Civ. 3777 (AKH)

ALVIN K. HELLERSTEIN, U.S.D.J.:

Intellectual Ventures II LLC ("Intellectual Ventures") sues JP Morgan Chase & Co. ("JPMC") for infringement of U.S. Patent No. 7,634,666 (the "'666 Patent"), which claims hardware, referred to as a "crypto-engine," capable of executing two public key encryption protocols. Document discovery concluded on April 10, 2015 and the parties have taken some, but not all, depositions. Prior to the completion of the deposition phase of discovery, JPMC moved for summary judgment based upon non-infringement. I hold that Intellectual Ventures has raised triable issues of fact and deny JPMC's motion.

I. Background

A. The '666 Patent

The '666 Patent claims a physical co-processor, referred to as a "crypto-engine," used to assist a host processor, such as a personal or network computer, with the encryption of data. Two aspects of the claimed hardware are particularly relevant. First, the crypto-engine has a Modular Arithmetic Unit capable of "heterogeneous computation," which means it can execute cryptographic algorithms at a higher speed than that at which the host processor operates. The crypto-engine contains an Interface Control Unit that moderates between the host processor and the Modular Arithmetic Unit, synchronizing the two asynchronous speeds.

Second, the claimed Modular Arithmetic Unit has the capability of executing two commonly-used public key encryption protocols known, respectively, as Rivest-Shamir-Adleman ("RSA") and Elliptic Curve Cryptography ("ECC"). RSA involves the computation of two large prime numbers whereas ECC involves computation based upon points on an elliptic curve. The Modular Arithmetic Unit's selection of the RSA or ECC protocols is based upon an op-code signal generated by a unit known as the "cryptographic controller." According to the patent specification, prior art was unable to conduct such "assymetic cryptographic algorithms" because "in known hardware architecture resources cannot be shared by the algorithms and reused." '666 Patent at 1:5-28; 2:49-63.

Intellectual Ventures alleges infringement of Claim 4 of the '666 Patent, which reads in relevant part as follows:

> A crypto-engine for cryptographic processing of data comprising an arithmetic unit operable as a co-processor for a host processor and an interface controller for managing communications between the arithmetic unit and host processor . . . the interface controller including: a bus interface for connecting high frequency manipulated data inside the arithmetic unit with the lower frequency manipulated data in the host processor; a concatenator/splitter for merging or splitting data width, and a cryptographic controller generating status and interrupt signals for the host processor and *generating an op-code signal for the arithmetic unit, the arithmetic unit selecting RSA or [ECC] modes of operation based on the op-code signal.*

'666 Patent at 11:43-12:19 (emphasis added). The parties primarily dispute the meaning and scope of the italicized clause. The Court previously construed "op-code signal" to mean a "[s]ignal capable of indicating an RSA operation when it has one characteristic and an ECC operation when it has a different charactistic." Order Regarding Claim Construction and Patent Summaries ("Markman Order"), No. 13 Civ. 3777, ECF No. 82 (S.D.N.Y. Mar. 18, 2014).

B. The Accused Product

Intellectual Ventures accuses the IBM 4765 PCIe Cryptographic Coprocessor (the "IBM Crypto Card") of infringing the '666 Patent. *See* Decl. Brent P. Ray Supp. Defs.' Mot. Summ. J. Based Upon Noninfringement ("Ray Decl."), Exh. D at 285. The parties dispute the functionality and capability of the IBM Crypto Card.

According to Intellectual Ventures, the IBM Crypto Card contains a unit known as the module central processing unit ("MCPU"), which purportedly operates as the crypto-graphic controller described in Claim 4 of the '666 Patent. *See* Decl. Sal Lim Supp. Pl.'s Opp'n Defs.' Mot. Summ. J. Based Upon Noninfringement ("Lim Decl."), Exh. C ¶ 23. In addition, the IBM Crypto Card contains a microchip known as "Otello," which purportedly operates as the arithmetic unit described in Claim 4. *See id.* ¶ 24. The MCPU is capable of receiving requests from the host processor to carry out either RSA or ECC public key encryption functions. *See id.*, Exh. C ¶¶ 26-29, Exh. G, Exh. N, Exh. Z. The MCPU then generates op-codes for use by Otello. *See id.* Although not sent to Otello directly, the op-code signals are generated by the MCPU for the sole purpose of instructing Otello to perform a RSA or ECC function. *See id.*, Exh. C ¶¶ 26-32, 35, Exh. G, Exh. N, Exh. Z. Based upon these op-code signals, Otello performs either RSA or ECC functions. *See id.*, Exh. C ¶¶ 29, 33, 35, Exh. Z. Intellectual Ventures argues that this satisfies the language of Claim 4 because the MCPU "generat[es] an op-code signal for" Otello and Otello "select[s] RSA or [ECC] modes of operation based on the op-code signal." '666 Patent at 12:17-19; *see* Opp'n Br. at 9.

JPMC disputes Intellectual Ventures' description of the IBM Crypto Card. First, JPMC asserts that while Otello performs RSA and several other mathematical functions, it does not perform ECC operations. *See* Corrected Mem. Law Supp. Defs.' Mot. Summ. J. ("Opening Br.") at 9; Ray Decl., Exh. C at 21, Exh. E ¶ 3. When ECC capability was added to the IBM Crypto Card in September 2010, it was added by updating software executed by the MCPU, and not by reconfiguring Otello's hardware. *See id.*, Exh. E ¶ 6. Thus, it is the MCPU, and not Otello, that is capable of performing ECC operations. *See id.* Furthermore, the MCPU does not send an op-code signal directly to Otello and, therefore, Otello's selection of the ECC operation cannot be based on the op-code signal as required by Claim 4. *See id.*, Exh. F ¶ 8; Opening Br. at 11.

II. Standard of Review

"The court shall grant summary judgment if the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a); *Celotex Corp. v. Catrett*, 477 U.S. 317, 322 (1986). A genuine issue of material fact exists "if the evidence is such that a reasonable jury could return a verdict for the nonmoving party." *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986). In ruling on a motion for summary judgment, the court must view all evidence in the light most favorable to the nonmoving party, *see Overton v. N.Y. State Div. of Military & Naval Affairs*, 373 F.3d 83, 89 (2d Cir. 2004), and must "resolve all ambiguities and draw all permissible factual inferences in favor of the party against whom summary judgment is sought," *Sec Ins. Co. of Hartford v. Old Dominion Freight Line Inc.*, 391 F.3d 77, 83 (2d Cir. 2004).

III. Discussion

The parties first dispute the scope of the claim language. JPMC argues that Claim 4 is limited to actual functionality (i.e., how the accused product performs in practice), rather than capability (i.e., potential uses of the accused product). Therefore, the argument continues, evidence that the IBM Crypto Card does not select or execute an ECC algorithm in practice establishes non-infringement as a matter of law. *See* Opening Br. at 4-6. Intellectual Ventures counters that the '666 Patent claims the capability of executing ECC algorithms and that the IBM Crypto Card has such capability. Thus, the argument goes, whether the IBM Crypto Card actually executes ECC algorithms, as opposed to RSA algorithms, is irrelevant. *See* Mem. Law Supp. Pl.'s Opp'n Defs.' Mot. Summ. J. Based on Noninfringement ("Opp'n Br.") at 9-13.

The extent to which capability alone may constitute infringement depends upon the scope and construction of a patent's claim language. *See Fantasy Sports Props., Inc. v. Sportsline.com, Inc.*, 287 F.3d 1108, 1117-18 (Fed. Cir. 2002) (noting that capability to infringe does not establish *per se* infringement because "in every infringement analysis, the language of the claims, as well as the nature of the accused product, dicates whether an infringement has occurred"); *see also Fujitsu Ltd. v. Netgear Inc.*, 620 F.3d 1321, 1329 (Fed. Cir. 2010) ("Unless the claim language only requires the capacity to perform a particular claim element, we have held that it is not enough to simply show that a product is capable of infringement."). For example, in *Typhoon Touch Technologies., Inc. v. Dell, Inc.*, upon which JPMC relies heavily, the district court, after reviewing the specification, expressly construed the claim at issue "as requiring that a device, to be covered by the claim, actually performs, or is configured or programmed to perform, each of the functions stated in the claim." 659 F.3d 1376, 1380 (Fed. Cir. 2011). After affirming the district court's claim constructions, the Federal Circuit held that summary judgment for non-infringement was appropriate because the apparatus was not configured to perform the recited function, as required by the district court's claim construction.[1] *See id.*

Unlike the district court in *Typhoon Touch*, I did not construe Claim 4 of the '574 Patent as being limited to actual performance. *See* Markman Order at 12 (construing "op-code signal" as a "[s]ignal *capable* of indicating an RSA operation when it has one characteristic and an ECC operation when it has a different charactistic") (emphasis added). Furthermore, the specification makes clear that the '666 Patent is broad enough to encompass hardware that is capable of performing ECC operations. For example, it recites that "the invention relates to a crypto-engine *capable of* executing either [RSA] or [ECC] public key encryption protocols." '666 Patent at 1:8-11 (emphasis added). Later, it recites that "[t]he preferred embodiment of the present invention provides a compact crypto-engine *capable of* executing assymetic cryptographic algorithms including both RSA and ECC protocols." '666 Patent at 2:59-63 (emphasis added). Nothing in the claim language limits the claimed hardware to actual performance of the claimed function. Rather the '666 Patent claims an "arithmetic unit selecting RSA *or* ECC modes of operation." '666 Patent at 12:18-19 (emphasis added).[2]

[1] In *Typhoon Touch*, the Federal Circuit drew a distinction between the capability of a device to perform functions recited by a patent, even in the absence of actual performance, and the need to modify or reprogram a device in order for it to have the capability of performing the recited functions. *See Typhoon Touch*, 659 F.3d at 1380-81. Depending on the scope of a patent's claim language, capability may constitute infringement, while the need for reconfiguration or reprogramming generally forecloses infringement claims. *Compare Microprocessor Enhancement Corp. v. Texas Instruments, Inc.*, 520 F.3d 1367, 1375 (Fed. Cir. 2008) ("[The claim] is clearly limited to a pipelined processor possessing the recited structure and capable of performing the recited functions.") *with Telemac Cellular Corp. v. Topp Telecom, Inc.*, 247 F.3d 1316, 1330 (Fed. Cir. 2001) ("[T]hat a device is capable of being modified to operate in an infringing manner is not sufficient, by itself, to support a finding of infringement.").

[2] *Nazomi Communications, Inc. v. Nokia Corp.*, 739 F.3d 1339 (Fed. Cir. 2014), upon which JPMC also relies, is similarly inapposite. In that case, the district court "construed the claims as claiming an apparatus, comprising both hardware and software, capable of practicing the claimed functionality. *Id.* at 1343. Because at the time of the alleged infringement the device lacked the software necessary to perform the functions claimed by the patent, the Federal Circuit affirmed summary judgment on the basis of non-infringement. *See id.*

Intellectual Ventures has presented evidence, sufficient to raise a triable issue of fact, that the IBM Crypto Card has the capability of selecting between RSA and ECC functionality.[3] For example, the data sheet for the IBM Crypto Card states that it contains "[h]ardware to perform . . . large number modular math functions for RSA (up to 4096-bit), ECC Prime Curve and other public-key cryptographic algorithms." Lim Decl., Exh. F at 1; *see also id.*, Exh. H at IBM-JPMC-0041962. Additionally, an IBM hardware engineer testified at his deposition that a chip within the IBM Crypto Card's arithmetic unit performs "either RSA or ECC." *Id.*, Exh. G at 46:3-15; *see also id.* at 18:1-9 ("It is true that the hardware supports large modular math functions for RSA. And the same modular math functions can be used for ECC as well.").

JPMC further argues that the IBM Crypto Card does not infringe the '666 Patent because there is no evidence that the MCPU "sends" op-code signals directly to Otello. *See* Opening Br. at 11-12. However, neither Claim 4 nor this Court's construction of the claim language are so narrow. Rather, the '666 Patent encompasses an arithmetic unit that selects either RSA or ECC protocols "based on" a generated op-code signal. '666 Patent at 12:15-19; Markman Order at 12. Intellectual Ventures has pointed to evidence, sufficient to raise a triable issue of fact, that the IBM Crypto Card is capable of such functionality. *See, e.g.*, Lim Decl., Exh. C ¶¶ 47-49. Accordingly, I similarly decline to grant summary judgment on this basis at this stage of the proceedings.

While it may prove to be true, in the end, that the IBM Crypto Card requires reconfiguration to infringe the '666 Patent or that the hardware itself is incapable of doing so, the

[3] In the alternative, Intellectual Ventures argues that there may be evidence that the IBM Crypto Card actually performs ECC cryptography but that JPMC's failure to place a litigation hold on relevant evidence resulted in spoliation. This is the subject of a separate motion pending before the Court and is scheduled to be fully briefed by July 7, 2015.

evidence presented thus far is sufficient to defeat JPMC's motion for summary judgment at this stage. I note that depositions and expert discovery may shine additional light on the functionality and capability of the IBM Crypto Card and JPMC may renew its motion for summary judgment following the close of discovery.

IV. Conclusion

For the foregoing reasons, JPMC's motion is DENIED. The Clerk shall mark the motion (Doc. No. 388) terminated. The stay of discovery imposed at the May 21, 2015 status conference, *see* Order Summarizing May 21, 2015 Status Conference, No 13 Civ. 3777, ECF No. 406 (S.D.N.Y. May 21, 2015), is hereby lifted. Fact discovery shall be completed by September 15, 2015, the same date as fact discovery related to the '574 Patent is scheduled to be complete. The status conference scheduled for August 10, 2015 is cancelled. A status conference on the two remaining patents in dispute shall be held on September 17, 2015 at 11:00 a.m.

SO ORDERED.

Dated: New York, New York
June 30, 2015

ALVIN K. HELLERSTEIN
United States District Judge